IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

LABMD, INC.	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 1:19-cv-852
	)	
	)	**TRIAL BY JURY**
THE PRIVACY INSTITUTE	)	**IS DEMANDED**
BRIAN J. TARQUINIO	)	
ROBERT J. BOBACK	)	
TIVERSA HOLDING CORP.	)	
REED SMITH, LLP	)	
	)	
-and-	)	
	)	
JARROD D. SHAW	)	
	)	
Defendants.	)	
	)	

COMPLAINT

Plaintiff, LabMD, Inc. ("LabMD"), by counsel, pursuant to Rule 3 of the Federal Rules of Civil Procedure (the "Rules"), files this action against Defendants, The Privacy Institute ("Privacy Institute"), Brian J. Tarquinio ("Tarquinio"), Robert J. Boback ("Boback"), Tiversa Holding Corp. ("Tiversa"), Reed Smith, LLP ("Reed Smith"), and Jarrod D. Shaw ("Shaw"), jointly and severally.

LabMD seeks (a) compensatory damages, statutory damages (three-fold the damages sustained) and punitive damages in the sum of **$150,350,000.00**, (b) prejudgment interest on the principal sum awarded by the Jury from February 25, 2008 to the date of Judgment at the rate of six percent (6%) per year pursuant to § 8.01-382 of the

Virginia Code (1950), as amended (the "Code), (c) reasonable attorney's fees in a sum to be determined by the Court, but not less than **$2,858,023.35**, pursuant the rule of law announced by the Virginia Supreme Court in *Burruss v. Hines* and Rule 54(d)(2) of the Federal Rules of Civil Procedure, and (d) court costs – arising out of Defendants' malicious prosecution, business conspiracy, and aiding and abetting.

LabMD also requests the entry of an Order piercing the corporate veil of the Privacy Institute and compelling Boback and Tarquinio to pay the Judgment entered in this action against the Privacy Institute.

I. INTRODUCTION

1. This is a case about conspiracy and corruption that killed the business of a small and highly successful cancer-detection laboratory.

2. In 2007, Tiversa and agents of the Federal Trade Commission ("FTC") embarked on a clandestine, cooperative mission to hack and shake down law-abiding American citizens. After the Federal Bureau of Investigation ("FBI") gave Tiversa a proprietary law enforcement surveillance tool, known as "enhanced peer-to-peer software" ("EP2P"),[1] Tiversa used that government surveillance technology to hack and gain unlawful access to protected computers on the Internet. Tiversa stole files from those computers containing, *inter alia*, consumers' federally-protected, private health and personal information. Tiversa altered the metadata on those files, and fabricated claims that the files had been "exposed" and were "found" by Tiversa on the Internet. Tiversa

[1] "The FBI developed EP2P as an investigatory tool. Its source code is closely held; it is not shared with or accessible to the agents who use the program, let alone the public." *United States v. Chiaradio*, 684 F.3d 265, 276-77 (1st Cir. 2012). EP2P is a "marvel" of modern technology that was "customized to assist in child pornography investigations". *Id.*

then tried to sell "remediation" services to the companies that it had illegally hacked using the FBI's surveillance software, EP2P. Tiversa falsely represented that it could fix the putative flaws in the companies' data security programs that led to the files being "exposed". For companies, such as LabMD, who refused to pay or be shaken down, Tiversa, without probable cause and with spite, ill-will and actual malice, turned those companies in to the FTC's attorney/investigators, so the FTC could prosecute those innocent companies for violating the Federal Trade Commission Act (the "FTC Act"), Title 15 U.S.C. § 45(a).[2]

3. On February 25, 2008, Tiversa illegally hacked into a LabMD computer and stole a 1,718-page LabMD insurance aging report ("insuranceaging_6.05.071.pdf") with federally-protected personal health information on over 9,000 patients (the "1718 File"). Insurance aging reports were generated by LabMD's billing department to show accounts receivable that had not been paid and so that billing staff could attempt to collect payments on outstanding claims from patients' insurance companies. The June 2007 insurance aging report (1,718 File), unlawfully hacked by Tiversa using the FBI surveillance tool, contained personal information, such as names, dates of birth, Social Security numbers ("SSNs"),

[2] Section 5(a) of the FTC Act declares unlawful "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). It empowers and directs the FTC "to prevent persons, partnerships, or corporations … from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." *Id.* § 45(a)(2). In its complaint against LabMD, the FTC alleged that LabMD's data security program was inadequate and thus constituted an "unfair act or practice" under Section 5(a) of the FTC Act. The FTC's entire case was predicated upon Tiversa's intentional falsehoods and misrepresentations. The FTC knew that Tiversa had broken the law. Instead of dismissing its complaint and apologizing to LabMD, however, the FTC, acting in concert with Tiversa, proceeded full-steam ahead. The malicious prosecution and conspiracy between Tiversa and the FTC destroyed LabMD's business.

current procedural terminology ("CPT") codes, and health insurance company names, addresses, and policy numbers, for approximately 9,300 patients of LabMD's physician clients.

4. As a result of their commercial use of EP2P to hack LabMD's computer and their possession and disclosure of the 1,718 File, Boback and Tiversa committed multiple federal and state crimes, including, without limitation, violations of Title 42 U.S.C. § 1320d-6 (Unlawful Possession and Use of Personal Health Information). Boback and Tiversa instigated and cooperated in the FTC enforcement action at issue in this action in order to cover-up their many crimes.

5. In May 2008, Boback and Tiversa began contacting LabMD to try to sell Tiversa's remediation services to LabMD.

6. In these conversations, Boback lied to LabMD. Boback misrepresented that it had "found" the 1718 File on a peer-to-peer ("P2P") file-sharing network, through a file sharing application called "LimeWire".[3] Boback further misrepresented that he "continued

[3] LimeWire was a free P2P file sharing client for Windows, OS X, Linux and Solaris operating systems. LimeWire used the gnutella network as well as the BitTorrent protocol to share and distribute content, primarily music, on the Internet. In 2010, the United States District Court for the Southern District of New York entered an injunction against LimeWire ruling that the platform intentionally caused a "massive scale of infringement" by permitting the sharing of thousands of copyrighted works by its 50 million monthly users. *Arista Records, LLC et al. v. Lime Wire, LLC*, Case 1:06-cv-05936 (S.D.N.Y.) (Document 334 – Consent Injunction)]. Peer-to-peer file-sharing applications, such as LimeWire, enable one computer user to make a request to search for all files that have been made available for sharing by another (or "host") computer that is also using the file-sharing application. In order for a searcher using LimeWare to receive a search result for LabMD's "insuranceaging_6.05.071.pdf" file, he or she would have to enter the search terms "insuranceaging" or "6.05.071". Both of those searches are highly unusual, and it is extremely unlikely that any LimeWire user would ever enter them, demonstrating that the 1,718 File was hacked by someone who was not using LimeWire. **Tiversa did not use LimeWire to steal the 1,718 File. It used EP2P**. *See United States v. Chiaradio*, 684 F.3d 265, 276 (1st Cir. 2012) (EP2P differs from LimeWire in at least three ways).

to see individuals [on peer-to-peer networks] searching for and downloading copies" of the 1718 File, *i.e.* that the 1,718 had "spread" across peer-to-peer networks.[4]

[4] Tiversa employed the same fraudulent means, methods and practices to secure contracts from the United States Government. In February 2009, Boback appeared on the *Today Show* and staged a "real-time" search of P2P networks, pretending that he had "discovered" the tax returns of U.S. citizens on computers in four different countries. In truth, Boback had remotely accessed Tiversa's datastore. He created the appearance of conducting a search and "finding" sensitive documents on the Internet. Boback leveraged his lies and deception to secure a contract with the Department of the Treasury. Tiversa secured work with the United States House of Representatives in a similar way. In 2009, details of confidential Ethics Committee investigations were "found" on a P2P-enabled computer. Tiversa falsely claimed that the information at issue had "spread" through the Internet and that Tiversa had found the report on computers in Washington, D.C., New York and London. [*See* https://www.computerworld.com/article/2528771/leaked-house-ethics-document-spreads-on-the-net-via-p2p.html]. On May 5, 2009, Boback testified before the House Subcommittee on Commerce, Trade and Consumer Protection. He stated that "[i]n February of this year [2009], Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One." What Congress and the American public never knew, however, was that the information was not downloaded by anyone in Iran. Instead, Boback instructed Wallace to find an IP address in Iran that could be used to perpetrate the fraud. Wallace found an address, and Boback proceeded to testify falsely before Congress that Marine One's information was found there. On July 29, 2009, Boback testified before the House Oversight and Government Reform Committee. In his written testimony, Boback repeated that he had conducted a "live demonstration" for NBC's *Today Show*, where "Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P." [https://republicans-oversight.house.gov/wp-content/uploads/2012/01/20090729Boback.pdf]. In his oral testimony, Boback misrepresented that Tiversa had found "the entirety of the U.S. nuclear information, all of our facilities, everything … [W]e found this in France, in four locations in France." [https://www.govinfo.gov/content/pkg/CHRG-111hhrg54009/html/CHRG-111hhrg54009.htm]. Tiversa also habitually defrauded private clients in Virginia. In 2008, Tiversa obtained documents from Wagner Resource Group, that included Social Security numbers of the firm's clients, including Supreme Court Justice Stephen Breyer. The documents were only found on the computer of a secretary of the firm, who had downloaded LimeWire. Boback directed Wallace to falsify a "spread" and informed Phylyp Wagner, the founder of the firm, of the "breach." Wagner contracted with Tiversa to provide mitigation services for $10,000 per month based upon Boback's fraudulent statements. Boback then directed Wallace to contact the *Washington Post*; to use a fake name; and to inform the Post reporter (Brian Krebs) that Justice Breyer's personal data was all over the Internet. Krebs published an article entitled, "**Justice Breyer Is Among Victims in Data Breach Caused by File Sharing**". [http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997.html].

7. When LabMD did not immediately engage Tiversa to perform "remediation" of the alleged "breach", Boback reminded LabMD that there were state "breach" laws that required "immediate notification of the affected individuals". Boback feigned empathy: "I know this breach is troubling." Boback provided copies of the *Washington Post* article about Virginia-based Wagner Resource Group [http://www.wagnerrg.com/], implying and insinuating that the LabMD "breach" would be reported to the press unless LabMD cooperated and hired Tiversa. Boback and Tiversa eventually attempted to extort LabMD. Tiversa threatened to report LabMD to the FTC, if LabMD did not pay Tiversa to "remediate" the alleged leak of the 1,718 File. After LabMD refused to pay and refused to be extorted, Tiversa reported LabMD to the FTC, instigating a full-blown enforcement action.

8. Fueled and instigated by Tiversa's lies, the FTC purported to "investigate" LabMD for three-and-one half (3½) years.

9. The FTC investigation began in 2009. At the request of Tiversa, the FTC issued a civil investigative demand ("CID") to the Privacy Institute[5] to produce copies of

[5] The Privacy Institute was incorporated on June 3, 2009. At all times relevant to this action, it was a shell corporation used to perpetrate fraud upon LabMD. Boback asserts that the Privacy Institute was created for the "singular purpose" of responding to the FTC CID. Boback claims that in 2009 Tiversa was in negotiations to sell its business to a public company. Boback did not want the CID to interfere with those negotiations. Tarquinio, on the other hand, advises that the Privacy Institute was "an entity that was established to take bids for either part or all of Tiversa if a company wanted to purchase them." According to Tarquinio, Boback did not inform Tarquinio that the Privacy Institute was set up to transmit information to the FTC. The FTC agreed to issue the CID to the newly-formed Privacy Institute. Sometime in 2009, prior to issuance of the CID, Tiversa transferred the stolen 1,718 File to the Privacy Institute. The FTC did not question Tiversa's use of the Privacy Institute. FTC officials clearly knew that the information was, in fact, coming from Tiversa, despite the use of the Privacy Institute. The FTC admitted that the use of Tiversa's information was unusual relative to standard agency operating procedures for enforcement measures.

documents containing personally identifiable and sensitive information about consumers that was "publicly available"[6] on peer-to-peer (P2P) file sharing networks. In response to the CID, the FTC obtained from Tiversa a list of companies/persons whose files Tiversa had "found" on the Internet. Tiversa called the list "FTC List71609". The list identified LabMD and the 1,718 File.

10. In the fall of 2009, representatives of Tiversa, including Boback, met with FTC staff (including a member of the FTC's trial team in the enforcement action that would be filed) in Washington, D.C., to discuss Tiversa's response to the CID. After the meeting in Washington, D.C., the FTC instructed Tiversa to manipulate and alter metadata on the 1,718 File. FTC attorney, Alain Sheer ("Sheer"), expressed concern about the Fourth Amendment implications if it was ever discovered that Tiversa had actually obtained the 1,718 File from a U.S. Citizen (LabMD) by hacking computers using the FBI's surveillance tool.

11. In 2012, then-FTC Commissioner J. Thomas Rosch sternly warned against relying on information provided by Tiversa. Commissioner Rosch stated that "Tiversa is more than an ordinary witness, informant, or 'whistle-blower.' It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations." [*See, e.g.*, Dissenting Statement of Commissioner J.

---

[6] Without EP2P, Tiversa would never have hacked into LabMD's computer, would never have stolen the 1718 File, and would never have been able to manufacture the false claim that the 1,718 File was "publicly available". The fact that Tiversa could only find the 1718 File with the illegal use of proprietary law enforcement surveillance software is proof, in and of itself, that the 1718 File was never "publicly available".

Thomas Rosch, FTC File No. 1023099 (June 21, 2012) at 1. https://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./1023099-labmd-full-commission-review-jtr-dissent.pdf].

12. FTC staff did not heed then-Commissioner Rosch's warning, and also did not follow his advice. Instead, acting in concert with Tiversa, FTC complaint counsel chose to further commit to and increase its reliance on Tiversa. In the summer of 2013, the FTC informed Tiversa that the 1,718 File needed to be found someplace other than Georgia – in other words, there needed to be "spread". The FTC advised Tiversa that it needed "more than one computer location" in order to prosecute a case against LabMD. Boback and Tiversa manufactured a document to satisfy the FTC's stated needs. The FTC subpoenaed deposition testimony and documents from Tiversa. Boback testified that the 1,718 File "has been found on a public P2P network as recently as November 2013. It has been downloaded from four different Internet Protocol ('IP') addresses, including IP addresses with 'unrelated sensitive consumer information that could be used to commit identity theft." Boback's testimony concerning the "spread" of the 1,718 File between 2008 and 2013 was knowingly false.[7]

13. On August 28, 2013, the FTC commenced a prosecution of LabMD under Section 5 of the FTC Act. The FTC charged that LabMD failed to provide "reasonable and appropriate" security for personal information maintained on LabMD's computer networks, and that this conduct "caused or is likely to cause" substantial consumer injury.

[7] In November 2013, Tiversa provided the FTC a document containing four (4) additional IP addresses on which Tiversa claimed that it found the 1,718 File. Tiversa produced this document in response to a subpoena issued by the FTC. The document – which was used by the FTC as part of its prosecution of LabMD – was a complete fabrication and forgery manufactured at Boback's direction.

The FTC contended that LabMD was liable for "unfair" acts or practices under § 5(a) of the FTC Act.

14. In May 2015, during the trial of the FTC's enforcement action against LabMD, a former Tiversa employee and whistleblower, Rick Wallace ("Wallace"), testified under criminal immunity that Tiversa's business model was to "monetize" documents that it downloaded from peer-to-peer networks, by using those documents to sell data security remediation services to the affected business, including (a) by representing to the affected business that the business' information had "spread" across the Internet via peer-to-peer sharing networks, when such was not necessarily the case, and (b) by manipulating Tiversa's internal database of peer-to-peer network downloads (which Tiversa called the "Data Store") to make it appear that a business' information had been found at IP addresses belonging to known identity thieves. Wallace further testified that these practices were followed with regard to Tiversa's discovery of LabMD's 1718 File. Wallace revealed that in order to retaliate against LabMD for refusing to purchase Tiversa's services, Tiversa reported its "discovery" of the 1718 File to the FTC, and that, at the direction of Boback, Wallace had manipulated Tiversa's Data Store to make it appear that the 1718 File had been found at four IP addresses, including IP addresses of known identity thieves. Wallace confirmed that he had fabricated a list of those IP addresses, which the FTC introduced into evidence during the enforcement action as CX0019.

15. CX0019 purports to show that Tiversa had downloaded the 1718 File from four (4) IP addresses on particular dates and times. Wallace created CX0019, at Boback's direction, in 2013, near the time of Boback's deposition in the FTC enforcement action, to make it appear that the 1718 File had "spread" to IP addresses belonging to known identity

thieves, and that the 1718 File had not been found at an Atlanta IP address, when, in fact, none of this is true. Boback specifically asked Wallace to include a San Diego IP address. Although it was not true, Wallace included on CX0019 the IP address 173.16.83.112 as one of the IP addresses where the 1718 File had been found because that IP address belonged to an individual in Apache Junction, Arizona, that Wallace believed to be an identity thief, based on data in Tiversa's Data Store indicating that the individual at that address possessed over 3,000 tax returns that he appeared to be selling. Tiversa had approximately twenty (20) IP addresses that it would use when making it appear as if files had been "spread" across the Internet, including to identity thieves. Some IP addresses were used more frequently than others. For example, Tiversa knew of IP addresses that had gone "dead" after law enforcement took action. If Tiversa claimed the 1718 File was found at one of these long-gone addresses, such as the IP address at Apache Junction, there would be no way to contradict Tiversa's claim.

16. The 1718 File was never found at any of the four (4) IP addresses listed on CX0019.

17. Wallace's trial testimony established that Tiversa's malicious scheme was premeditated; that Tiversa acted out of a desire to hurt LabMD after LabMD refused to pay for Tiversa's services; that Tiversa hacked LabMD's file directly from a LabMD computer, and lied about it; and that Tiversa falsified the evidence the FTC used to prosecute LabMD.

18. Wallace's astounding revelations would and should have caused any ethical and moral attorney in the pursuit of justice to drop the enforcement action immediately, and apologize. However, Boback/Tiversa and the FTC refused to end their conspiracy to malicious prosecute LabMD.

19. On November 15, 2015, the Administrative Law Judge found in favor of LabMD.

20. In his written decision, the Administrative Law Judge made the following findings of fact:

> 157. Mr. Boback was motivated to retaliate against LabMD for LabMD's refusal to purchase remediation services from Tiversa, including by making the disclosure of the 1718 File appear widespread and dangerous. (F. 115-118, 126, 128-130, 148-154).
>
> 158. Mr. Boback's motive to retaliate against LabMD for refusing to purchase remediation services from Tiversa (F. 157) resulted in Tiversa's decision to include LabMD in the information provided to the FTC in response to the FTC CID (F. 137) and in the creation of CX0019. (F. 141-144, 146-149).
>
> 159. CX0019 is not credible or reliable evidence to show that the 1718 File spread on any peer-to-peer network. (F. 156-158).
>
> 160. Because of Mr. Boback's biased motive, Mr. Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of Respondent. (F. 156-159).

21. After FTC Commissioners reversed their own Administrative Law Judge,[8] LabMD appealed the Commissioners' ruling to the United States Court of Appeals for the Eleventh Circuit.

---

[8] Although the FTC Commissioners disregarded the findings of the Administrative Law Judge, the Commissioners unanimously agreed that Boback had perjured himself:

> "We concur with the ALJ's conclusions that the testimony of Robert Boback, CEO of Tiversa, was not credible or reliable. In particular, we agree that Mr. Boback's assertion that Tiversa had gathered evidence showing that the 1718 file had spread to multiple Internet locations by means of LimeWire was false and that the document that purported to list Internet locations where the 1718 file had been found (CX0019) was unreliable."

In the Matter of LabMD, Inc., 2016 FTC LEXIS 128, *91 (F.T.C. July 28, 2016) (citations to record omitted), *vacated*, *LABMD, Inc. v. FTC,* 894 F.3d 1221 (11th Cir. 2018).

22. During oral argument on July 3, 2017 before the United States Court of Appeals for the Eleventh Circuit in *LabMD v. FTC*, Case No. 16-16270, the Court of Appeals expressed particular concern about Tiversa and its sordid dealings with the FTC:[9]

> THE COURT: Mr. Hoffman [FTC's Appellate Counsel], is there – is there any concern on the part of the government how this information was imparted to the FTC? This company, Tiversa, doesn't come in here with clean hands, does it?
>
> MR. HOFFMAN: Well, certainly Tiversa has engaged in some misconduct in connection with the –
>
> THE COURT: Was there collusion between Tiversa and the government?
>
> MR. HOFFMAN: No.
>
> THE COURT: Well, Counsel, let me put it this way. What – the aroma that comes out of the investigation of this case is that Tiversa was shaking down private industry with the help of the FTC, will go to the – with the threat of going to the FTC. 'If you don't cooperate we will go to the FTC.' It may well be how they got some of their clients. But that's – that's an aroma that – and with falsifications to the Commission. The Administrative Law Judge just shredded Tiversa's presentation, just totally annihilated it.
>
> MR. HOFFMAN: I'm sorry. I mean –
>
> THE COURT: I – I – and –
>
> MR. HOFFMAN: So, I mean, what's – what's – what's – what's – what's the question?
>
> THE COURT: That – that was a – just a – just an observation.
>
> …
>
> MR. HOFFMAN: So I – I mean, my – my … my observation is that – is that … Tiversa – Tiversa's conduct is not really what's at issue here. I mean, there's no question … that Tiversa engaged in serious, serious misconduct in connection with this –

[9] An audio recording of the oral argument in the referenced appeal is available at http://www.ca11.uscourts.gov/oral-argument-recordings. The transcribed portions quoted herein begin at 23:18 and end at 25:30.

THE COURT: No, and got the Commission involved in their – in their shakedowns.

MR. HOFFMAN: I – I don't – I don't agree with that.

THE COURT: Oh, Counsel. Come on.

MR. HOFFMAN: I don't agree with that.

THE COURT: Oh, you – I know, you can't agree with it. But it should have become obvious after … the evidence collapsed and your – and complaint counsel couldn't go any further.

23. On June 6, 2018, the United States Court of Appeals for the Eleventh Circuit vacated the decision of the FTC Commission.

24. The FTC did not appeal, ending LabMD's 10-year odyssey.

25. The FTC prosecution of LabMD ended in a manner favorable to LabMD.

26. LabMD brings this action to recover for the special injuries and other losses caused by the malicious prosecution of the FTC enforcement action instigated by and with the cooperation of the Defendants.

II. PARTIES

27. LabMD is a corporation organized under the laws of the State of Georgia. It was founded in 1996. Its principal place of business was Atlanta. The sole shareholder, President and CEO of LabMD is Michael J. Daugherty ("Daugherty"). Daugherty is a citizen of Virginia. Daugherty controls the business and affairs of LabMD from his place of business within the Alexandria Division.

28. Between 2001 and 2014, LabMD was in the business of conducting clinical laboratory tests on urological specimen samples from patients and reporting the test results to its physician customers. LabMD provided uro-pathology cancer detection services to urologists who wanted their patients' tissue samples analyzed by pathologists who

specialized in prostate cancer or bladder cancer. During the period LabMD was operational, LabMD tested samples from patients in multiple states. The patients whose samples LabMD tested and from whom LabMD collected payments were located throughout the United States, including Virginia.

29. Given the nature of its work, LabMD was subject to data-security regulations issued under the Health Insurance Portability and Accountability Act of 1996, known colloquially as "HIPAA". LabMD was a "covered entity" under HIPAA. [https://privacyruleandresearch.nih.gov/pr_06.asp; https://www.cms.gov/regulations-and-guidance/administrative-simplification/hipaa-aca/areyouacoveredentity.html]. LabMD maintained and employed a data-security program in an effort to comply with those regulations.[10]

30. LabMD's business was very successful. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately $35-40 million. LabMD's peak annual revenue was approximately $10 million. From 2005 through 2012, LabMD's approximate blended profit margin was 25%. In 2013, LabMD's revenue was approximately $2 million. In January 2014, LabMD began winding down its operations. At that time, LabMD stopped accepting specimen samples and conducting tests. By letter dated January 6, 2014, LabMD notified its physician clients that it would not be accepting new specimens after January 11, 2014, and that all test results would be provided in the following week. LabMD further told its physician clients that LabMD would be closed for

[10] LabMD's program included a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections.

telephone calls and internet access after January 15, 2014, and that for the remainder of 2014, requests for past results or to obtain specimens for second opinions, could be made by facsimile. As of the start of the evidentiary hearing in the FTC enforcement action in May 2014, LabMD's operations were limited to preserving tissue samples for LabMD's physician clients, so the physicians could send out slides for second opinions, and to providing test results to physicians if they did not have them.[11]

31. Defendant, Privacy Institute, is a Delaware corporation. Privacy Institute is a dummy, stooge, alter ego and instrumentality of Defendants Tarquinio and Boback that was created solely to perpetrate fraud on LabMD and to aid, abet and facilitate Boback and Tiversa's malicious prosecution of LabMD. Boback asked his financial advisor, Tarquinio, to be the President of the Privacy Institute. Tarquinio accepted the request as a favor to Boback. Tarquinio is a money manager for UBS. *See, e.g.*:

http://financialservicesinc.ubs.com/team/wtlgroup/meetourteam.html;

http://financialservicesinc.ubs.com/fa/briantarquinio/index.html;

https://www.linkedin.com/in/brian-tarquinio-138a52/.

In 2009, Tarquinio managed a portfolio of investments for Boback and/or Tiversa. The Privacy Institute was, at all relevant times, undercapitalized and insolvent. It paid no dividends. Boback and Tarquinio commingled the Privacy Institute's corporate affairs with their personal affairs; disregarded corporate formalities; and failed to maintain corporate records. The officers and directors of the Privacy Institute, if they had any, were completely non-functional. Upon information and belief, the sole officer, director and

[11] LabMD is no longer in clinical operation, but still exists as a company and continues to secure its computers and the patient data stored within them from Virginia.

shareholder (on paper only) was Tarquinio. The Privacy Institute's "principal office" was Tarquinio's office at UBS. The Privacy Institute had no employees; it had no bank accounts; and conducted no business except for acting as a conduit to transfer files and information to the FTC. The Privacy Institute was dissolved on June 18, 2013. On the certificate of dissolution, the address for Tarquinio is that of Boback's uncle.

32. Defendant, Tiversa, is or was a Delaware corporation. Tiversa is no longer operational. Tiversa was a "P2P intelligence" company that offered data breach detection and remediation services to clients it blackmailed. On its website (no longer operational), Tiversa claimed that its "patented technologies" allowed it to conduct 1.8 billion searches on 500 million computers every day. At all times relevant to this action, Tiversa transacted continuous business in Virginia and derived substantial income from that business. Among Tiversa's largest Virginia customers was the Transportation Security Administration ("TSA").[12]

33. Defendant, Boback, is a citizen of Florida. He was a chiropractor. His medical license was suspended indefinitely shortly after he founded Tiversa in 2004. [https://www.dos.pa.gov/ProfessionalLicensing/LicensingServices/2005/ChiropracticOctober2005.pdf]. Boback lived in the Pittsburgh area until the FBI raided Tiversa headquarters on March 1, 2016.

34. In July 2007, Boback hired Wallace as a "forensic engineer" and analyst. Wallace's job as a forensic engineer included searching for exposed files on peer-to-peer

[12] To obtain the contract with the TSA, Boback falsely reported to the TSA that information about sensitive checkpoint and security measures had been found on computers in Yemen, Columbia and Kenya. In fact, the file was found only at a single computer, attributable to a TSA employee and located within the United States.

networks, and recording the information disclosed, including the company that had the disclosure, and when the information was disclosed. This information would be included on a spreadsheet that Tiversa analysts would update several times a day. The purpose of the spreadsheet was so that Boback and the Tiversa sales force could make sales calls to the affected companies. When Wallace, or any other analyst at Tiversa, downloaded a file that was deemed significant, Boback would be advised, and Boback would make the decision as to how to proceed to "monetize" the file; *i.e.*, whether the information would be given to a salesperson, or whether Boback himself would contact the company, to try to sell Tiversa's services. Tiversa would monetize information it obtained from peer-to-peer networks either by selling a monitoring contract, pursuant to which Tiversa would search for certain key words for a period of time, or by selling a "one-off" service, that would remediate just the existing disclosure problem. A Tiversa monitoring services contract for a large financial company could cost as much as a million dollars per year, down to a few thousand dollars per month for monitoring contracts for small "mom and pop" companies. When a company refused to purchase Tiversa's services, Boback would often respond, in reference to that company, to the effect of, "you think you have a problem now, you just wait." Thereafter, an analyst of Tiversa would input information into Tiversa's Data Store so as to make that company's information "proliferate" in Tiversa's Data Store and thereby make it appear that a file had "spread" to multiple places. Tiversa could use this Data Store "evidence" to follow up with a company to try again to get the company to purchase Tiversa's remediation services. When a company refused to purchase Tiversa's services after being contacted by Tiversa about a disclosure, Tiversa would need an excuse to make contact with the company again, so it would contact the company to report that the file had

proliferated, or "spread," to additional IP addresses, including IP addresses of known "bad actors" or identity thieves. Part of Wallace's job for Tiversa was to make it appear that a company's file had "spread" to more IP addresses, including to IP addresses of identity thieves. He did this by placing files he might have found outside Tiversa's searching system into a folder in the Data Store and making it appear that Tiversa had located and downloaded the file from the IP address of a known bad actor. As far as the Data Store sees it, the file was downloaded from that IP address, but in reality no data transferred.

35. Defendant, Reed Smith, is a limited liability partnership. None of Reed Smith's partners is a citizen of Georgia. Reed Smith is an international law firm with offices throughout Virginia, including Richmond and Tysons (McLean), Virginia:

https://www.reedsmith.com/en/offices/richmond;

https://www.reedsmith.com/en/offices/tysons.

36. Defendant, Shaw, is, upon information and belief, a citizen of Pennsylvania.

37. One or more agents of the FTC who conspired with Privacy Institute, Boback and Tiversa to prosecute LabMD, including lead prosecutor, Laura R. VanDruff ("VanDruff"), and Carl H. Settlemyer, Jr. ("Settlemyer"), who actively undertook the malicious prosecution at issue, live and/or work in Virginia. A substantial part of the events or omissions giving rise to LabMD's claims occurred in Virginia.

III. JURISDICTION AND VENUE

38. The United States District Court for the Eastern District of Virginia has subject matter jurisdiction over this action pursuant to Title 28 U.S.C. § 1332. The parties are citizens of different States and the amount in controversy exceeds the sum or value of $75,000, exclusive of interest, costs and fees.

39. The Defendants are subject to personal jurisdiction in Virginia pursuant to Virginia's long-arm statute, § 8.01-328.1(A)(1), (A)(3) and (A)(4) and § 8.01-328.1(B) of the Code, as well as the Due Process Clause of the United States Constitution. They are subject to both general and specific personal jurisdiction in Virginia. They engaged in continuous and systematic business in Virginia. They conspired with citizens of Virginia to harm LabMD. They have minimum contacts with Virginia such that the exercise of personal jurisdiction over them comports with traditional notions of fair play and substantial justice and is consistent with the Due Process Clause of the United States Constitution.

40. Venue is proper in the Alexandria Division of the United States District Court for the Eastern District of Virginia pursuant to Title 28 U.S.C. § 1391(b)(1) and (b)(2).

IV. STATEMENT OF ADDITIONAL MATERIAL FACTS

41. In order to perpetrate its crimes on LabMD and others, including businesses located in Virginia, Tiversa used several tools to search for and download computer files. Tiversa never sought permission and never had authority at any time to access LabMD's protected computers or to download any files on those computers. Tiversa obtained and converted information from protected computers, including those belonging to LabMD, even though it knew that most of what it searched for, found and downloaded was never intended to be shared by the owners of the computers it hacked.[13]

[13] Tiversa's actions in hacking LabMD's computers violate § 1030(a)(2)(C) of the Computer Fraud and Abuse Act ("CFAA"), Title 18 U.S.C. § 1030(a)(2)(C), and numerous other federal and state civil and criminal laws including, without limitation, Title 42 U.S.C. § 1320d-6 (Unlawful Possession and Use of Personal Health Information) and § 18.2-152.3 of the Virginia Code (Computer Fraud).

42. One of the tools used by Tiversa to search for, access and download files on the Internet was a software program Tiversa called "Eagle Vision".

43. Another tool used by Tiversa to search for, access and download files was EP2P – the FBI proprietary law enforcement surveillance software and hardware tool owned by the United States Government (the "FBI Surveillance Tool").

44. In approximately 2007, the Pittsburgh Office of the FBI installed a dedicated FBI-only DSL line on a Tiversa computer, so that Wallace could use the FBI Surveillance Tool to search for, access and download files from protected computers. Upon information and belief, the FBI never authorized Tiversa to hack LabMD's computer; never knew that Tiversa had done so; and knew nothing about Boback and Tiversa's arrangement with the FTC or their efforts to extort money from LabMD and other businesses in Virginia and elsewhere.

45. The FBI Surveillance Tool was not owned or developed by Tiversa. The Tool is owned by the United States Government and is used by the FBI primarily for investigating child pornography. The FBI Surveillance Tool had more capabilities to search for, access and download files from peer-to-peer networks than standard off-the-shelf peer-to-peer software programs, such as LimeWire. Boback and Tiversa used the FBI Surveillance Tool to steal the 1,718 File from LabMD.

46. At all times relevant to this action, Privacy Institute, Tarquinio, Boback, Tiversa, Reed Smith, Shaw, and the FTC each knew that Tiversa's illegal practice of accessing and taking files from protected computers without authorization or permission violated numerous Federal and State laws.

47. Attorney/investigators at the FTC, who were responsible for the relationship with and use of Tiversa, include, but are not limited to, Sheer, Ruth Yodaiken, Settlemyer and VanDruff. In 2007, Tiversa began acting in concert with these persons to unlawfully access protected computers for the purpose of obtaining consumer data that the FTC hoped would lead to prosecutions under the FTC Act.

48. Tiversa used the FBI Surveillance Tool to assist the FTC in identifying potential enforcement targets. Tiversa also used the Government surveillance software for its own commercial purposes and for commercial gain, including stealing the 1,718 File from LabMD and using the 1,718 File to extort money from LabMD.

49. On May 13, 2008, Boback called LabMD to inform it that Tiversa had "found" LabMD's 1718 File on the Internet and that Tiversa was available to help LabMD remediate the alleged "leak" of the File. Boback lied to LabMD and fraudulently concealed the fact that Tiversa had used the FBI Surveillance Tool to surreptitiously hack directly into a LabMD protected computer to steal the 1718 File from LabMD.

50. After Tiversa's initial call, LabMD duly investigated and determined that, unbeknownst to LabMD, LimeWire was installed on a LabMD billing computer. Upon discovery in May 2008, LabMD removed the LimeWire application immediately.

51. Boback's May 13, 2008 call to LabMD was the first act in a series of aggressive efforts to intimidate and coerce LabMD into purchasing Tiversa's "remediation" services. Tiversa also used attorneys and threats to coerce LabMD into hiring Tiversa. On November 21, 2008, for instance, Jim Cook, an attorney hired by Tiversa's chairman of the board, Joel Adams, misrepresented to an attorney for LabMD that Tiversa was "concerned" that it had to report its "finding" of the 1718 File to the FTC.

Cook's implicit threat to turn LabMD into the FTC did not motivate LabMD to hire Tiversa.

52. When Boback learned that Daugherty refused to do business with Tiversa, Boback said to Wallace, "F--- him. Make sure he's at the top of the list" for investigation by the FTC. The "list" was a spreadsheet that Tiversa was preparing for the FTC that included the names of companies whose files had been stolen by Tiversa and who refused to hire Tiversa to remediate Tiversa's breaches (the "List"). The List included public companies, banks, schools, numerous health providers, insurers, etc. Most of the names on the List did business in Virginia.

53. Tiversa's scheme was the same for each company on the List. Tiversa hacked confidential files from those companies, sent the stolen files to the potential "customers", told the potential customers, fraudulently, that the disclosed files had spread to additional computers on the internet, including computers of known bad actors (*i.e.*, identity thieves), and tried to extort the companies into buying Tiversa's services.

54. The FTC, Privacy Institute, Boback, Tiversa, Reed Smith and Shaw combined, associated and acted together for the purpose of maliciously prosecuting LabMD for violation § 5(a) of the FTC Act. Tiversa's phone records are telling of the company's relationship with the FTC, and proof that the parties acted in concert. The phone records indicate that Tiversa employees placed two phone calls to FTC attorney VanDruff in June 2008, and, in the four months between March 2009 and July 2009, Tiversa employees called Sheer at his FTC office on 21 occasions. Boback was one of the FTC's main contacts at Tiversa prior to July 2009. Regular phone calls between Tiversa and the FTC took place between August 2009, when Tiversa provided information to the

FTC through the Privacy Institute, and January 2010, when the FTC sent letters to nearly all of the companies Tiversa and the Privacy Institute turned over to the FTC, including LabMD. During these six (6) months, Tiversa employees called Sheer 34 times.

55. Boback and Tiversa had special advance knowledge that the FTC intended to prosecute LabMD and other the companies identified in the documents and information turned over by the Privacy Institute in response to the CID. Boback and Tiversa acquired this insider information from the FTC. Armed with material non-public information and knowledge of these impending FTC actions, Tiversa maneuvered to position itself to profit from the FTC's actions. In the fall of 2009, Boback began working with LifeLock, a major partner of Tiversa and Tiversa's largest source of income, to send letters to the companies that would be contacted by the FTC – the very companies that Tiversa turned over to the FTC. In October 2009, Boback e-mailed senior LifeLock executives about the impending FTC investigations. Boback explained that the *Washington Post* planned to "shame" companies into addressing the problem, and that the upcoming FTC investigations presented a unique opportunity for LifeLock and Tiversa to profit. In early October 2009, Boback advised LifeLock that "the FTC letters did not go out yet so the companies will not know what you are talking about … yet." He further advised that LifeLock should "suggest Tiversa if asked by the company".

56. By letter dated January 19, 2010, FTC attorney Sheer informed LabMD that the FTC was "conducting a non-public inquiry into LabMD's compliance with federal law governing information security." Sheer's letter states, "[a]ccording to information we have received, a computer file (or files) from your computer network is available to users on a peer-to-peer file sharing ('P2P') network (hereinafter, 'P2P breach')." The source of

Sheer's false statement was Tiversa. In truth, in 2010 when Sheer wrote the letter, **no LabMD files were available to anyone** using peer-to-peer file sharing software. LabMD had removed the offending LimeWire from its billing computer in May 2008. Sheer knew that LabMD found and removed the offending software the day Tiversa contacted LabMD in 2008. Before he penned the January 19, 2010 letter, Sheer knew that Tiversa was the only source of the 1,718 File. There was no probable cause or plausible reason for the FTC to investigate LabMD – the 1718 File was not available or "spreading" anywhere and there was no substantial injury as required by 15 U.S.C. § 45(n).[14]

57. On February 22, 2010, the FTC publicly announced that it had notified "almost 100 organizations" about data breaches that occurred on peer-to-peer file sharing networks, and that it had opened non-public investigations into several other companies. https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe]. Boback sent the link to executives at LifeLock. LifeLock responded, "Once again you guys are at the top of the food chain. Any problem with us pushing this with media and using you?" Boback promptly replied, "No problem."

58. Boback could not have known the details of the FTC's investigations – including the timing of the January 2010 letters, which constituted pre-decisional information about pending non-public government actions – without some sort of inside information concerning the FTC's enforcement plans. The insider tips, upon information and belief, came from Sheer and VanDruff. It is clear that Tiversa and the FTC shared a

[14] In truth, the FTC knew that Tiversa's files were falsified and doctored prior to the investigative letters going out to nearly 100 companies in January 2010. Tiversa stole the files, doctored them, then the FTC told Tiversa to doctor them a different way by striping the metadata completely out.

common goal and had a mutually beneficial relationship. As a Congressional Oversight Committee would conclude in 2015, "**the FTC used Tiversa as the source of convenient information used to initiate enforcement actions, and Tiversa used the FTC to in further pursuing the company's coercive business practices**." (Emphasis added).

59. In early (spring) 2010, Boback told Wallace that the FTC was concerned with the collection of information on U.S. citizens and that it was better to leave that type of data out.

60 In approximately July 2010, Boback advised Wallace to create "spread" regarding LabMD and to show additional IP addresses where the 1,718 file was allegedly found. Wallace used three (3) IP addresses that Tiversa previously connected to fraud/criminal activity and provided those IP addresses to Boback. Wallace also had to create and store records in Tiversa datasets in what was commonly referred to as the "storeroom". Wallace created records making it appear he had found the 1,718 File at three other locations (IPs) and altered date/time stamps (also referred to as "metadata") as well as filenames to make it appear that he found the LabMD records on those three IPs around the same period as he found the records at the Atlanta location.

61. Wallace had done something like this before for Boback. At Boback's direction , Wallace had created records to make it look like some Pentagon/DoD documents had been found in China.

62. Wallace considered fabrication of IP addresses and the alteration of metadata to be "dirty" work.

63. On December 22, 2011, the FTC served LabMD with a CID.

64. LabMD moved to quash the CID, but was not successful.

65. On July 19, 2013, Daugherty posted a promotional trailer on the Internet for a new book, *Devil Inside the Beltway* – a book Daugherty had written about his 3 ½ year ordeal with Tiversa and the FTC. The book, which was published in mid-September 2013, exposed Tiversa's theft of the 1718 File, the confidential relationship between the FTC and Tiversa, and the FTC and Tiversa's abuse and destruction of Daugherty's small cancer detection laboratory.

66. Upon review of Daugherty's trailer for *Devil Inside The Beltway*, the FTC retaliated, ended its "investigation" and, within a month, began prosecution of LabMD based upon the documents and information supplied by Privacy Institute, Boback and Tiversa.

67. Tiversa's use of the FTC as a retaliatory weapon against LabMD was extremely costly, disruptive and harmful to LabMD and Daugherty, causing substantial special damages and actual damages. However, the FTC prosecution afforded LabMD the right to take certain discovery from Boback, Tiversa and the FTC, and thereby expose: (1) Boback, Tiversa and the Privacy Institute's instigation of the FTC investigation and subsequent prosecution; (2) Boback and Tiversa's collusion with the FTC; (3) Boback, Tiversa and the Privacy Institute's fraudulent business practices; (4) Boback and Tiversa's lies regarding the 1718 File; and (5) Boback and Tiversa's illegal use of the FBI Surveillance Tool to spy on and steal from American citizens, including LabMD (collectively the "Concealed Misconduct").

68. In response to the threat of exposing the Concealed Misconduct and to prevent LabMD from succeeding in its battle against the FTC, Boback and Tiversa escalated their malicious efforts to harm LabMD. Boback and Tiversa (a) terminated

Wallace, who refused to lie for Tiversa in the FTC's enforcement action; (b) hired private investigators (CSI and InPax) to investigate, intimidate, harass, photograph, track, trail, antagonize and surveil witnesses and their family members to prevent witnesses from testifying against Boback and Tiversa; (c) contacted the Gartner Group, Black Hat and other organizers of events where Daugherty would be speaking to defame and impugn the character of Daugherty and LabMD in order to undermine LabMD and Daugherty and ruin their reputations; (d) directed Tiversa employee, Keith Tagliaferri ("Tagliaferri"), to create a false report regarding the "spread" of the 1718 File and submit that false report to Congress during a congressional investigation into the sordid relationship between Tiversa and the FTC; (e) coordinated efforts with and assisted the FTC in its prosecution of LabMD; (f) gave false testimony (Boback) in two depositions in the FTC's enforcement action; (g) interfered with LabMD's efforts to obtain immunity against prosecution for Wallace – a Whistleblower; (h) with the assistance of their non-Government lawyers, Reed Smith and Shaw, published and republished lies about LabMD, including, without limitation, February 10, 2015 statements published in the Pathology Blawg and December 9, 2015 statements published in The Wall Street Journal, and lies about Tiversa's "finding" the 1718 File on the computers of known bad actors, all in an effort to assist the FTC in the prosecution of LabMD; (i) fabricated supporting evidence for the FTC to use in its prosecution of LabMD; (j) coerced Tiversa chief technology officer, Anju Chopra, to sign a materially misleading affidavit; and (k) upon information and belief, conspired with former United States Attorney, Mary Beth Buchanan, to conceal Tiversa's illegal use of the FBI Surveillance Tool.

69. On September 5, 2013, Boback wrote and sent an internal email to Tiversa employees, Dan Kopchak and Molly Trunzo. In the email, Boback admitted the following facts:

> "In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name "LabMD" in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."

70. In or about October 2013, Boback directed Wallace to create another document showing "spread" of the 1,718 File to be sent to the FTC. Boback told Wallace that this document needed to show that the 1,718 File had been found at a San Diego IP address, not an Atlanta address. Boback also told Wallace to modify the date on the document to show that the 1,718 File had been found in San Diego in February 2008. Boback stood over Wallace as Wallace fabricated the document. Boback gave the document to the FTC and the FTC used the document as an exhibit (CX0019) in its prosecution of LabMD.

71. Reed Smith and Shaw actively aided and abetted Boback and Tiversa in the malicious prosecution of LabMD. Reed Smith and Shaw actively and regularly communicated and collaborated with the FTC on behalf of Boback and Tiversa. By letter dated October 17, 2013 to LabMD's counsel, Reed Smith and Shaw misrepresented the following:

> "[T]he evidence will indisputably show that Tiversa and Mr. Boback did not access, take, 'invade' or ever obtain the File through a LabMD computer."

Reed Smith and Shaw knew this statement was false. Boback's September 5, 2013 email in Reed Smith and Shaw's possession proved that Tiversa downloaded the 1718 File directly and only from a LabMD computer in Atlanta, Georgia, on February 25, 2008. In

the same October 17, 2013 letter, Reed Smith and Shaw repeated the fabricated story about Tiversa finding the 1718 File on a computer in San Diego:

> "Moreover, the evidence will also show that [Boback and Tiversa] accessed the File through a computer located in San Diego – and not the LabMD Computer – with an Internet Protocol Address of 68.107.82.250. Thus, any and all statements asserting or implying that the Plaintiffs accessed the File through a LabMD computer are demonstrably incorrect."

Shaw and Reed Smith knew this statement was false and that Boback had fabricated evidence of the "spread".

72. In furtherance of the scheme to maliciously prosecute LabMD under the FTC Act, Reed Smith and Shaw also aided and abetted the concealment of evidence. On November 1, 2013, in response to a subpoena served on Tiversa by the FTC, Shaw and Reed Smith produced documents to FTC attorney, VanDruff, under a cover letter marked "Private and Confidential." Even though the subpoena called for its production, Shaw and Reed Smith concealed the September 5, 2013 email in which Boback admitted that Tiversa downloaded the 1718 File directly from LabMD's computer. Instead, Shaw and Reed Smith produced the document, admittedly fabricated by Wallace (CX0019), purporting to show that Tiversa located and downloaded the 1718 File (with file name "insuranceaging_6.05.071") from four (4) computers on the internet at the following IP addresses and on the following dates and times:

IP Address	***Date***	***Time***
68.107.85.250	02/05/2008	@ 3:49pm
173.16.83.112	11/05/2008	@ 11:26pm
201.194.118.82	4/7/2011	@ 2:22am
90.215.200.56	6/9/2011	@ 8:13am

The document produced by Shaw and Reed Smith to the FTC was embraced and used by the FTC in its enforcement action against LabMD. It is infamous Exhibit CX0019. The

FTC used the false evidence in this document to argue that LabMD allowed the 1718 File to spread through cyberspace.

73. Reed Smith and Shaw also produced four (4) copies of the 1718 File to the FTC, representing that each had been downloaded from the IP locations in CX0019. These representations were knowingly false.

74. CX0019 and the four (4) copies of the 1718 File produced by Shaw and Reed Smith were created by Tiversa and Boback to deceive Administrative Law Judge, Michael D. Chappell, who presided over the FTC's enforcement action against LabMD, and to help the FTC prevail over LabMD at any cost.

75. In addition to the fabrication of evidence, Boback, Tiversa, Reed Smith and Shaw concealed an internal document proving that Tiversa downloaded the 1718 File directly and solely from a LabMD computer in Atlanta.

76. On or about April 18, 2008, Tiversa prepared and sent to its client, CIGNA, a forensic report regarding the 1718 File (the "CIGNA Report"). The CIGNA Report states that "[a]fter reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that LabMD near Atlanta, Georgia is the disclosing source [of the 1718 File]."

77. On November 21, 2013, Boback knowingly and falsely testified in the FTC enforcement action that Tiversa found the 1718 File on computers at the four (4) locations identified in CX0019. Boback falsely testified that the computers were located in San Diego, California; Apache Junction, Arizona; London, England; and San Jose, Costa Rica. In furtherance of the FTC's position, Boback testified that those computers were known to have been used by identity thieves and other bad actors.

78. On January 30, 2014, LabMD served a subpoena on Wallace for a deposition to be taken in the FTC enforcement action. Boback told Wallace that he must lie at his deposition and not disclose the Concealed Misconduct. Boback cornered Wallace in an elevator at work and told him, "This is what you are going to say in your deposition so that our stories match." Wallace told Boback he would not lie under oath. Boback responded by saying, "No, this is what you are going to say." Boback went so far as to pull out his firearm, point it at Wallace and threaten to harm Wallace if he revealed the Concealed Misconduct.

79. In February 2014, Boback threatened Wallace that he would cancel Wallace's insurance if he (Boback) was not given access to Wallace's medical records. In an effort to tamper with, harass and intimidate Wallace, to prevent Wallace from disclosing the Concealed Misconduct, and to assist the FTC in its prosecution of LabMD, Boback called Wallace's health care provider and falsely represented that Wallace was a rogue employee who had been on probation many times over the course of his employment. In yet another violation of 42 U.S.C. § 1320d-6 (Unlawful Possession and Use of Personal Health Information), Boback and Tiversa gave a copy of Wallace's medical records to the police, and told the police to "keep an eye" on Wallace.

80. On February 26, 2014, Shaw informed LabMD's counsel that Wallace was "no longer available" to be deposed due to an "unexpected medical issue."

81. On April 2 and April 3, 2014, Wallace called Daugherty to blow the whistle on Tiversa and Boback. Wallace reported the following, *inter alia*, to Daugherty:

- Wallace resigned from Tiversa on April 1, 2014, after Boback demanded that Wallace lie under oath to the United States Government.

- The four IP addresses given to the FTC were not the sources of the 1,718 File.

- Boback lied when he stated under oath to the FTC that Tiversa found the 1718 File on four IP addresses and downloaded the File from a San Diego, California location, which is not a LabMD workstation IP address.

- The 1718 File was never found anywhere other than a LabMD computer.

82. At or around the time Wallace terminated his employment at Tiversa, Boback, Tiversa, Reed Smith and Shaw hired and directed private investigators, CSI Investigations, Inc. ("CSI") and Sam Rosenberg of InPax, to intimidate, harass, photograph, videotape, track, trail, antagonize, surveil and leave threatening notes for Wallace and his family. Tiversa, Boback, and their private investigators intimidated, harassed and threatened Wallace and his family in numerous ways in order to prevent Wallace from disclosing the Concealed Misconduct and to assist the FTC in its prosecution of LabMD. Examples of their misconduct include, but are not limited to, the following:

- On June 3, 2014, Wallace found a note on Tiversa letterhead in the refrigerator in his shed, which read, "ICU!"

- Also on June 3, 2014, the electrical cords on some of Wallace's power tools had been cut and their border collie dogs had been let out after Wallace's wife had locked them in the house.

- On the morning on June 26, 2014, Boback followed Wallace's car on 1-79 in Pittsburgh and began to alternate between passing Wallace, following Wallace, and slowing down in front of Wallace. Wallace tried to pass Boback who then tried to run Wallace off the road.

- On or about June 30, 2014, a Ford Crown Victoria pulled into Wallace's driveway. Two individuals who exited the car falsely claimed they were investigative agents and asked if they could come inside his home.

- In mid-July 2014, while Wallace's wife and the Wallace children were in Montana at a family reunion, the doorbell to the Wallace's home rang multiple times during the night. The Wallace's doorbell rang less frequently when Wallace's and the Wallace children were home, but it continued on a weekly basis. The doorbell stopped after Wallace testified before the FTC.

- The garage door to the Wallace home opened "on its own" randomly multiple times per day. The random garage door opening stopped after Wallace testified before the FTC.

- Boback and Tiversa had the Wallace home under surveillance. On or about November 8, 2014, a Tiversa IT employee told Wallace's wife that Boback had installed a camera on the Wallace's property and had been recording them. The employee said he saw the surveillance feed because he was asked to open a port on one of Tiversa's computers so that Boback could access the feed. The employee said the last images he had seen were of the Wallace's son getting out of the car at the end of the driveway. The son inadvertently stepped on the camera as he went to pick something up.

- On or about October 20, 2014, Wallace's wife found a note in the Wallace mailbox that read, "WATCH OUT."

- On April 15 or 17, 2015, about one month before Wallace was scheduled to testify as a witness for LabMD in the FTC enforcement action, Wallace saw that someone had written in pink chalk at the end of his driveway "U R DEAD."

- When Wallace and his wife arrived at the Mayflower Hotel just before Wallace's testimony in the FTC enforcement action, Ms. Wallace was told by the front desk attendant at the Mayflower Hotel that a "Mr. Boback" had canceled the reservation.

83. In early June 2014, in furtherance of the scheme to maliciously prosecute LabMD, Boback directed Tagliaferri to prepare a report containing false information regarding the alleged "spread" of the 1718 File (the "Tagliaferri Report"). The Tagliaferri Report contains, *inter alia*, the following false information:

> "The 6 additional IP addresses were detected in possession of the 1,718 page 'Insurance Aging' Report (insuranceaging_6.05.071.pdf) on various dates within the disclosure date ranges referenced above."

> "These 6 IP addresses possess additional files including federal tax returns relating to numerous individuals, credit reports. credit card and bank account statements, passports. Usernames and passwords to online accounts, medical patient data, lists of credit card numbers, social security numbers, instructions on how to hack and steal passwords etc. Tiversa classifies these 6 additional IP addresses as Information Concentrators."
>
> "Throughout our extensive P2P research, Tiversa continues to see individuals harvesting a large number of files containing confidential and sensitive data. Tiversa calls these individuals 'Information Concentrators' and in most cases, they are suspicious in nature … Information Concentrators gather this information and could potentially use it for malicious purposes."

84. The misconduct of Privacy Institute, Boback, Tiversa and the FTC did not go unnoticed by the United States Government.

85. In or around August 2014, the United States House of Representatives Oversight and Government Reform Committee (the "OGR Committee") initiated an investigation into the business practices of Tiversa and its relationship with the FTC.

86. On November 14, 2014, the United States Attorney issued Wallace a grant of immunity pursuant to 18 U.S.C. § 6002.

87. On April 20, 2015, Reed Smith and Shaw sent affidavits of Boback and Anju Chopra, Tiversa's chief technical officer, to VanDruff, FTC's lead counsel in the enforcement action against LabMD. Reed Smith and Shaw provided those affidavits to the FTC in furtherance of the prosecution of LabMD and in order to help the FTC discredit Wallace and to prove with false and misleading information and documents that Tiversa found and downloaded LabMD's 1718 File from computers at four (4) or more different locations on the Internet.

88. On May 5, 2015, Wallace testified under immunity in the FTC enforcement action. He disclosed the following bombshell facts:

- On February 25, 2008, Tiversa located the 1718 File on a LabMD computer near Atlanta, Georgia.

- Tiversa never found the 1718 File anywhere other than on a LabMD computer.

- In April 2008, Tiversa reported to CIGNA, one of its customers, that Tiversa had located LabMD's 1718 File on a LabMD computer at a LabMD IP address near Atlanta, Georgia.

- Tiversa reported the "disclosure" of the 1718 File to CIGNA in the hope that CIGNA would pressure LabMD to become a Tiversa client.

- It was Tiversa's practice to create Incident Record Forms for Boback and others at Tiversa to use as a list of prospective customers. Tiversa would make cold calls to the prospective companies to describe the "problem" the companies were having and to offer Tiversa's remediation services.

- At Boback's direction, Tiversa employees would manipulate the data in Tiversa's data repositories to make it appear that prospective customers' files had spread to other locations on the peer-to-peer networks. This was often done to give Boback a reason to contact a prospective customer again. Boback would report, for example, that a prospective customer's computer file had spread to computers owned by known identify thieves.

- Tiversa would never tell prospective customers where their files were found. Tiversa would claim that the IP address of the source computers were not recorded. Wallace said this was a lie – Tiversa always knew the IP addresses of the source computers.

- Wallace testified about the List (an exhibit marked as RX 551). Wallace explained that the companies on the List were chosen "so that the FTC would contact them and notify them of a data breach and hopefully we would be able to sell our services to them."

- In the fall of 2009, Boback, Wallace and other Tiversa employees travelled to Washington, D.C. to discuss the 1,718 File with the FTC.

- After their return from D.C., Boback contacted people on the List to tell them that the FTC would be taking action against them if they did not become Tiversa clients.

- Boback told Wallace to include LabMD on the List in retaliation for LabMD not hiring Tiversa.

- At some point before Boback's deposition in the FTC enforcement action on November 21, 2013, Boback told Wallace to change the data in Tiversa's Data Store to make sure that the 1718 File did not appear to have come from the Atlanta area. Boback directed Wallace "that under no circumstances can the insurance aging file originate from a Georgia IP address or an Atlanta area IP address. And in addition to that, [Boback] told [Wallace] to find an individual in San Diego to include with this list."

89. On May 15, 2015, Congressman Darrell E. Issa released a Staff Report from the House Oversight and Government Reform Committee ("OGR"), entitled, "*Tiversa, Inc.: White Knight or High-Tech Protection Racket?*" that was prepared on January 2, 2015 (the "OGR Report"). The key findings of the OGR Report are as follows:

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

Key Findings

- Rather than the cyber "white knight" Tiversa purports to be, the company often acted unethically and sometimes unlawfully in its use of documents unintentionally exposed on peer-to-peer networks.
- At least one Tiversa employee, under the direction of CEO Robert Boback, provided intentionally false information to the United States government on more than one occasion. Boback later provided false testimony about fabricated documents to the U.S. House of Representatives.
- According to a whistleblower, Tiversa fabricated that an Iranian IP address downloaded and disclosed the blue prints for the President's helicopter, Marine One. Tiversa allegedly did so in order to receive press attention for the company. The Committee found that statements made by Tiversa under oath about this matter could not be substantiated.
- After obtaining information on HIV/AIDS patients at a clinic in Chicago, Tiversa employees called the patients, purportedly in an attempt to get the clinic to hire Tiversa. When the clinic refused to hire Tiversa, the company gave the information to a lawyer that worked with the company who filed a class-action lawsuit that eventually settled for a substantial amount of money.
- Tiversa had information about a breach at the House Ethics Committee exposing information about investigations into Members of Congress. Tiversa did not return this information to the Ethics Committee and instead appears to have sought publicity for the leak.
- Tiversa's co-founder claims the company is in possession of a greater quantity of sensitive and classified information than NSA-leaker Edward Snowden.
- Information provided by Tiversa to the FTC through a shell organization known as the Privacy Institute was only nominally verified but was nonetheless relied on by the FTC for enforcement actions.
- Tiversa obtained non-public, advanced knowledge of FTC enforcement actions from which it attempted to profit.
- According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography and classified government documents.

90. The OGR Report contains the following conclusions regarding Boback and Tiversa's actions:

> During the course of this investigation, the Committee conducted ten day-long transcribed interviews and reviewed over 50,000 pages of documents. Documents and testimony obtained by the Committee in the course of its investigation displayed a troubling pattern with respect to Tiversa's business practices. Tiversa routinely provided falsified information to federal government agencies. Instead of acting as the "white knight" the company purports to be, Tiversa often acted unethically and sometimes unlawfully after downloading documents unintentionally exposed on peer-to-peer networks. At least one Tiversa employee, under the direction of Boback, provided intentionally false information to the United States government on more than one occasion. This is a crime. In addition, Boback provided false testimony about fabricated documents to the U.S. House of Representatives.

> Several years ago, Tiversa CEO Robert Boback began perpetrating a scheme in which at least one Tiversa employee manipulated documents legitimately found on the peer-to-peer network to show that the documents had spread throughout the peer-to-peer network. For example, Tiversa downloaded a file that computer A shared on a peer-to-peer network. The file could be copied and the metadata easily manipulated thoroughly widely-accessible computer software programs to make it appear that it had been downloaded by computers B, C, and D, and thus spread throughout the peer-to-peer network. Tiversa relied on the manipulated documents to create a need for their "remediation" services and to grow the company's reputation through press statements and manipulation of media contacts. Boback told media contacts that certain documents, including sensitive government documents, spread throughout the peer-to-peer network when in fact they had not.
>
> According to a whistleblower, Tiversa not only provided the manipulated information to its clients, but in some instances also provided false documents to various entities of the United States government, including the Congress and several agencies. Not only is this unethical, but it is illegal to give false information to the United States government.[3] It is also illegal to obstruct a congressional investigation by providing false information to a congressional committee.[4]

> Throughout this investigation, the Committee routinely found that information provided by Tiversa either could not be verified, or simply did not make sense. Part of the story always seemed to be missing. The whistleblower's testimony that Tiversa routinely falsified documents, however, filled in these gaps.

> Boback created a culture of intimidation at Tiversa. The Committee has unfortunately learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormely accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.[10] Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. The suit against Wallace effectively questions Mr. Wallace's Constitutional right to speak with Congress after the Committee approached him with questions related to allegations about Tiversa. These are clear instances of witness intimidation and interference with a congressional investigation on the part of Boback and Tiversa.

> Tiversa's interactions with the FTC raise questions about the propriety of the relationship. Both Tiversa and the FTC have characterized the relationship as nominal. Overwhelming evidence produced to the Committee, however, demonstrates mutually-beneficial collaboration, wherein the FTC obtained information validated its regulatory authority, and Tiversa gained an ally in a powerful federal agency that provided actionable information that it exploited for monetary gain. Unfortunately, this relationship existed at the expense of good government.
>
> The FTC accepted information from Tiversa through a shell organization without questioning the motives or reason for the third party, or, significantly, the veracity of the underlying information. The FTC's motives for blindly accepting this information are unclear.
>
> In addition, Tiversa's involvement with LabMD, a medical testing laboratory based in Atlanta, Georgia, raises questions. Not only does LabMD's story offer a case study illustrating Tiversa's coercive business practices and relationship with the FTC, but information the Committee obtained shows that Boback lied about material information in the case, which ultimately led to the shuttering of LabMD.

> In an internal e-mail dated almost three months before the deposition and never produced to the FTC, however, Boback stated that Tiversa downloaded the LabMD file while working for a client. He stated, "The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. This statement, made by Boback in September 2013, fundamentally calls into question his claim that Tiversa never downloaded the LabMD file from the IP address in Georgia.[226]

> Further, the initial report that Tiversa provided to a client about the LabMD document stated that the company first "observed" the LabMD file in San Diego, California on August 5, 2008.[227] Tiversa could not have downloaded the LabMD file from an IP address in San Diego in February 2008 if it did not even observe the file at this IP address until August 2008.

91. Despite Wallace's testimony in the FTC enforcement action, despite the clear and unimpeachable findings in the OGR Report, despite the FTC's recognition that CX0019 and Boback's testimony were false, and despite the September 5, 2013 email and

the CIGNA Report, Privacy Institute, Boback, Tiversa, Reed Smith and Shaw pressed forward with the malicious prosecution of LabMD.

92. The FTC prosecution of LabMD finally terminated in 2018. During the course of this malicious prosecution, Privacy Institute, Boback, and Tiversa committed multiple federal and state crimes:

a. It is a crime under 42 U.S.C. § 1320d-6(a) for a person to knowingly obtain or disclose individually identifiable health information relating to an individual if the information is maintained by a covered entity and the person obtained or disclosed such information without authorization. 42 U.S.C. § 1320d-6(b)(3) provides that if the offense is committed with intent to use individually identifiable health information for commercial advantage, the offender should be fined not more than $250,000, imprisoned not more than 10 years, or both.

b. It is a crime under 18 U.S.C. § 1030(a)(2)(C) to intentionally access a protected computer without authorization and to obtain information that computer, and a felony to do so for commercial advantage or private commercial gain.

c. It is a crime under 18 U.S.C. § 1001 to knowingly and willfully falsify, conceal or cover up "by any trick, scheme, or device a material fact"; to make "any materially false, fictitious, or fraudulent statement or representation"; or to make or use "any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry" in "any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States."

d. It is a crime under 18 U.S.C. § 1505 to "corruptly" "influence[], obstruct[], or impede[] or endeavor[] to influence, obstruct, or impede the due and proper

administration of the law under which any pending proceeding is being had before any department or agency of the United States…." The term "corruptly" means "acting with an improper purpose, personally or by influencing another, including making a false or misleading statement, or withholding, concealing, altering, or destroying a document or other information." 18 U.S.C. § 1515(b); *see also U.S. v. Blackwell*, 459 F.3d 739, 761-62 (6th Cir. 2006).

e. It is a crime under 18 U.S.C. § 1519 to "knowingly alter[], destroy[], … conceal[], cover[] up, falsif[y], or make[] a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States…."

f. It is a crime under 18 U.S.C. § 371 to conspire to do any of the acts enumerated in subparaghs a-e above.

93. Privacy Institute, Boback, and Tiversa violated 42 U.S.C. § 1320d-6(a), 18U.S.C. § 1001, 18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 1505, 18 U.S.C. § 1519, and 18 U.S.C. § 371.

COUNT I – MALICIOUS PROSECUTION

94. LabMD states a claim for malicious prosecution. More specifically, (a) Privacy Institute, Boback, Tiversa, Reed Smith and Shaw initiated, instigated and/or assisted and actively cooperated in the FTC enforcement proceeding against LabMD, (b) the proceeding terminated in a manner not unfavorable to LabMD, (c) the proceeding was instituted without probable cause, and (d) Privacy Institute, Boback, Tiversa, Reed Smith and Shaw acted with malice, out of a controlling motive other than a good faith desire to

further the ends of justice, enforce obedience to the FTC Act, suppress unlawful conduct, or see that the guilty are punished. *Stanley v. Webber*, 260 Va. 90, 95-96, 531 S.E.2d 311 (2000); *Giant of Virginia, Inc. v. Pigg*, 207 Va. 679, 684, 152 S.E.2d 271 (1967) (malice may be inferred from the lack of probable cause).

95. Privacy Institute, Boback, Tiversa, Reed Smith and Shaw's malicious prosecution of LabMD was egregious, vile and contemptuous, especially in light of the extreme efforts undertaken to lie under oath, fabricate evidence, suborn perjury, tamper with witnesses and obstruct justice.

96. Because of Privacy Institute, Boback, Tiversa, Reed Smith and Shaw's malicious prosecution, LabMD suffered substantial damage and incurred loss, including, but not limited to, special injuries, destruction of its business, financial injury and loss of good will, damage to its name and reputation, attorney's fees, and other out-of-pocket expenses in an amount to be determined by the Jury, but not less than $50,000,000.00.

97. As a result of Privacy Institute, Boback, Tiversa, Reed Smith and Shaw's malicious prosecution, LabMD seeks compensatory damages and punitive damages, as well as attorney's fees pursuant to the rule of law announced by the Virginia Supreme Court in *Burruss v. Hines*, 94 Va. 413, 26 S.E. 875, 878 (1897) ("The general rule is that counsel fees are not recoverable as damages; but on the trial of an action for malicious prosecution or false imprisonment, where exemplary damages are recoverable, the fees paid or incurred to counsel for defending the original suit or proceeding may be proved, and, if reasonable and necessarily incurred, may be taken into consideration by the jury in the assessment of damages.").

COUNT II – BUSINESS CONSPIRACY

98. Beginning in 2007 and continuing through June 2018, Privacy Institute, Boback, Tiversa, Reed Smith and Shaw, acting as individuals, combined, associated, agreed or acted in concert together and with agents of the FTC, including Sheer and VanDruff, for the express purposes of injuring LabMD in its trade and business. In furtherance of the conspiracy, the Defendants engaged in a joint scheme the unlawful purpose of which was to maliciously prosecute LabMD under the FTC Act. At all times during the course of the conspiracy, Reed Smith and Shaw acted illegally, fraudulently and outside the scope of their employment as attorneys for Tiversa and Boback.

99. The Defendants acted intentionally, purposefully, without lawful justification, and with the express knowledge (a) that Boback and Tiversa had committed multiple federal crimes when Tiversa hacked LabMD's computers and obtained and distributed the 1,718 File, (b) that the evidence supplied by Privacy Institute, Boback, and Tiversa was totally fabricated, and (c) that Boback had both committed perjury and suborned perjury in furtherance of the conspiracy to maliciously prosecute LabMD. Defendants acted with the express and malicious intent to injure LabMD and destroy its business.

100. The Defendants' actions constitute a business conspiracy in violation of § 18.2-499 of the Code.

101. As a direct result of the Defendants' willful misconduct, LabMD suffered damage and incurred loss, including, but not limited to, injury to its trade and business, injury to its reputation, attorney's fees, court costs, and other damages in the sum of $50,000,000.00 or such greater sum as is determined by the Jury.

102. In accordance with § 18.2-500 of the Virginia Code, LabMD seeks the recovery of three-fold the damages it sustained in the sum of $150,000,000.00.

COUNT III – AIDING AND ABETTING

103. The law recognizes a cause of action for aiding and abetting an intentional tort. *See, e.g., Tysons Toyota, Inc. v. Globe Life Ins. Co.*, 45 F.3d 428, at * (4th Cir. 1994) ("Under Virginia law, one who aids and abets a third party's breach of fiduciary duty may be held liable for providing such assistance") (citing *Patteson v. Horsley*, 70 Va. (29 Gratt.) 263, 270-271, 273, 276 (1877)); *Priester v. Small*, 2003 WL 21729900, at * 5 (Loudoun Cir. 2003) (recognizing a cause of action for aiding and abetting) (citing *Daingerfield v. Thompson*, 74 Va. (33 Gratt.) 136, 149-150 (1880) ("He who commands or procures another to do an unlawful act, is as responsible as a trespasser as he who commits the trespass.")); *Sherry Wilson and Co., Inc. v. Generals Court, L.C.*, 2002 WL 32136374, at * 1 (Loudoun Cir. 2002) ("On two occasions the Supreme Court of Virginia has recognized the right of an injured plaintiff to recover damages against person who aids and abets the principal actor. More recently, Judge Kathleen H. Mackay has found claim founded upon the aiding and abetting of a fraud was sufficient to withstand demurrer. *Kieft v. Becker*, 2002 Va. Cir. LEXIS 33 (Fairfax County 2002). Thus, unlike some jurisdictions, it may be said that the common law of the Commonwealth has looked with favor upon recovery in tort against those who aid and abet others in the commission of the civil wrong for which damages may be maintained."); *see Quinn v. Knight*, 2016 WL 6471462, at * 4 (E.D. Va. 2016) (even if the claim of aiding and abetting is not to be treated as a separate tort, "it appears to be a viable alternative theory to secure joint liability.") (citing *All. Tech. Group v. Achieve 1, LLC*, 2013 WL 143500, at * 5 (E.D. Va. 2013)).

104. Privacy Institute, Reed Smith and Shaw aided and abetted the malicious prosecution of LabMD, and are, therefore, jointly liable with Boback and Tiversa for that tort. *Sherry Wilson & Co., Inc. v. Generals Court, L.C.,* 2002 WL 32136374, at * 1 (Loudoun Cir. 2002) ("Complainant questions whether Virginia recognizes a separate tort action for aiding and abetting a fraud. On two occasions the Supreme Court of Virginia has recognized the right of an injured plaintiff to recover damages against person who aids and abets the principal actor. Thus, one who encouraged another to commit an assault could be held liable for the injury resulting from the other's actions. *Daingerfield v. Thompson,* 74 Va. (33 Gratt.) 136 (1880). Similarly, one who assists another to breach his fiduciary duty to the beneficiaries of a trust may be held jointly and severally liable for the losses sustained as a result of such breach. *Patteson v. Horsley,* 70 Va. (29 Gratt.) 263 (1877). More recently, Judge Kathleen H. Mackay has found claim founded upon the aiding and abetting of a fraud was sufficient to withstand demurrer. *Kieft v. Becker,* 2002 Va. Cir. LEXIS 33 (Fairfax County 2002), *See also Tysons Toyota, Inc. v. Globe Life Insurance Co.,* 1194 U.S.App. LEXIS 36692 (4th Cir. 1994)). Thus, unlike some jurisdictions, it may be said that the common law of the Commonwealth has looked with favor upon recovery in tort against those who aid and abet others in the commission of the civil wrong for which damages may be maintained. In order to recover damages against one who aids and abets in the commission of a fraud, it must be shown that not only the underlying fraud was committed but, "... that there was knowledge of this fraud on the part of the aider and abettor, and substantial assistance by the aider and abettor in the achievement of the fraud, and that damages to the plaintiff were proximately caused thereby." 37 Am.Jur.2d *Fraud and Deceit* § 302 (2002)); *see id. Priester v. Small,* 2003

WL 21729900, at * 5 (Loudoun Cir. 2003) ("while there is a difference of opinion between the judges of this Circuit as to the existence of the cause of action for aiding and abetting, this Court has previously ruled, consistent with the authorities set forth above, that such a cause of action exists.") (citing *Patteson v. Horsley*, 70 Va. (29 Gratt.) 263, 270 (1877) (one who assists another to breach his fiduciary duty to the beneficiaries of a trust may be held jointly and severally liable for the losses sustained as a result of such breach – "Any other disposition of any part of the trust subject made by the trustees in any other manner, was a breach of trust by them for which they were responsible, as also were any other persons who may have knowingly participated with them in such breach of trust."); *Daingerfield v. Thompson*, 74 Va. (33 Gratt.) 136, 149-150 (1880) ("It is no excuse or justification of Daingerfield to say that he did not fire the pistol which caused the injury. He was the aider and abettor and instigator of Harrison, who fired the fatal shot, and he, himself, admits that it was fired at his advice and instigation … The firing of the pistol was in itself an unlawful act, and advised and instigated by him, he must take the consequences of the result. He who commands or procures another to do an unlawful act, is as responsible as a trespasser as he who commits the trespass. *Jordan v. Wyatt*, 4 Gratt. 151. And although the act committed was done without malice, yet being unlawful, the party committing it or aiding or abetting in its commission, is responsible in damages to the party injured")); *Tysons Toyota, Inc. v. Commonwealth Life Ins.*, 1990 WL 10039336, at * 2 (Fairfax Cir. 1990) ("A defendant who aids and abets in the commission of a tort may be jointly liable for that tort, but he is not liable for a separate tort of aiding and abetting.").

105. Privacy Institute, Reed Smith and Shaw aided and abetted Boback and Tiversa's intentional tort of malicious prosecution by, *inter alia*, (a) receiving the stolen

1,718 File from Boback and Tiversa and transferring the stolen property to the FTC, (b) providing fabricated evidence to the FTC, and (c) by concealing documents from the FTC.

106. As a direct result of these Defendants' willful misconduct, LabMD suffered damage and incurred loss, including, but not limited to, injury to its trade and business, injury to its reputation, attorney's fees, court costs, and other damages in the sum of $50,000,000.00 or such greater sum as is determined by the Jury.

COUNT IV – PIERCING THE CORPORATE VEIL

107. Privacy Institute was the alter ego, alias, stooge, or dummy of Boback, Tarquinio and Tiversa. Privacy Institute was a device or sham created by Boback and Tarquinio for the sole purpose of facilitating, aiding and abetting the malicious prosecution of LabMD, disguising and obfuscating Boback and Tiversa's wrongdoing, obscuring Boback and Tiversa's fraud, and concealing Boback and Tiversa's crimes.

108. LabMD requests the entry of an Order piercing the corporate veil of the Privacy Institute, and imposing personal liability on Boback and Tarquinio for payment of the Judgment entered against the Privacy Institute in this action.

CONCLUSION AND REQUEST FOR RELIEF

WHEREFORE, LabMD respectfully request the Court to enter Judgment against the Defendants, jointly and severally, as follows:

A. Compensatory damages in the amount of $50,000,000.00;

B. Treble damages in the sum of $150,000,000.00;

C. Punitive damages in the amount of $350,000.00 or the maximum amount allowed by law;

D. Prejudgment interest at the rate of 6% per year on the Principal Sum awarded by the Jury from February 25, 2008 to the date of Judgment;

E. Postjudgment interest at the rate of six percent (6%) per annum until paid;

F. Reasonable Attorney's Fees and Costs;

G. Such other relief as is just and proper.

TRIAL BY JURY IS DEMANDED

DATED: June 26, 2019

LABMD, INC.

By: */s/ Steven S. Biss*

Steven S. Biss (VSB # 32972)
300 West Main Street, Suite 102
Charlottesville, Virginia 22903
Telephone: (804) 501-8272
Facsimile: (202) 318-4098
Email: stevenbiss@earthlink.net

Counsel for the Plaintiff